Observations in the Dissemination of Intelligence Surveillance and Reconnaissance (ISR) Data and Information within a Coalition Environment

Mr John L Mahaffey
NATO Consultation, Command and Control Agency
PO Box 174
2501 CD The Hague
The Netherlands

John.Mahaffey@nc3a.nato.int

True genius resides in the capacity for the evaluation of uncertain, hazardous, and conflicting information.

Winston Churchill

ABSTRACT

Intelligence Surveillance and Reconnaissance (ISR) Systems have become a leading edge capability for the Joint and Combined Forces Commander. The 21st century battlefield is characterized a varied level of threats, weapons and missions. These include large force conventional operations, special operations, counter-insurgency operations, anti crime operations and natural disaster relief. The threats run the gamut from well equipped conventional forces to poorly equipped insurgents; from terrorists equipped with weapons of mass destruction to disease brought on by natural disaster and famine. The commander must plan for this new battlefield with weapons, command and control and information. Much of this information, especially that received and exploited in near real time, comes from ISR assets. Unfortunately, ISR assets are both high demand and low density. No single nation can afford to provide all the ISR the commander needs. As a result, the commander must rely on a coalition of ISR systems to provide this benefit. But there are problems, information security, system interoperability, communications limitations and variable capabilities and limitations within ISR system classes conspires to reduce the overall system's effectiveness for use in near real time across a broad coalition. The Coalition Aerial Surveillance and Reconnaissance (CAESAR) project serves as the primary model for this experimentation. This paper will address some of these issues and provide potential solutions based upon experimentation with multinational ISR systems in a coalition environment. The data and information detailed in this paper are based upon an operational view of technical capabilities to disseminate ISR data across a multinational coalition.

1.0 INTRODUCTION

The headlines today read like a National Geographic magazine. Conventional war in the Middle East, civil war in Africa, natural disasters in South East Asia, illegal immigration in North America and counter narcotics in South America; as each crisis unfolds the requirement for military or governmental support closely follows. This support may come as a request for conventional military force, Special Forces, logistical support or para-military and police forces such as the Coast Guard and Customs. Each of these forces comes with specific mission support requirements. In many cases, these requirements are specific to the mission. For example, weapons requirements for a para-military force are vastly different than a

Mahaffey, J.L. (2005) Observations in the Dissemination of Intelligence Surveillance and Reconnaissance (ISR) Data and Information within a Coalition Environment. In *Analytical Support to Defence Transformation* (pp. 26-1 – 26-16). Meeting Proceedings RTO-MP-SAS-055, Paper 26. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
01 APR 2005

2. REPORT TYPE
N/A

3. DATES COVERED
-

4. TITLE AND SUBTITLE
Observations in the Dissemination of Intelligence Surveillance and Reconnaissance (ISR) Data and Information within a Coalition Environment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NATO Consultation, Command and Control Agency PO Box 174 2501 CD The Hague The Netherlands

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202031. NATO/RTO-MP-SAS-055, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
unclassified	**unclassified**	**unclassified**	**UU**	**16**	

large conventional force. Logistics requirements such as fuel, supply, transportation and housing are different for conventional military operations and civilian disaster relief. However, there is one common thread among all of these forces and missions; the need for rapid and reliable access to data and information that is both accurate and actionable.

1.1 Joint and Combined Forces – The Coalition

The Joint Forces/Combined Joint Task Force Commander (JFC/CJTF) faces an increasingly complex array of threats on the today's battlefield. The battlefield on which the JFC/CJTF must engage contains a growing number of traditional and non-traditional threats. These run the gamut from conventional armies to insurgents. During primarily civilian operations such as those supporting Tsunami relief in South East Asia, the threat may not be human at all. In these cases the threat may be disease and starvation. In many cases, these threats may present themselves simultaneously across both a linear and non-linear battlefield. The JFC/CJTF may be required to fight a conventional war, battle insurgents behind friendly lines and support the local population with medical and material assistance. Combating these threats requires the right mix of weapons and weapons systems, seamless command and control (C2) and current, accurate and actionable intelligence. Among these elements, C2 and intelligence particularly must be fused in such a way that commands at all levels can exploit and counter adversary intentions before they become a threat.

Traditionally, intelligence has been the purview an intelligence directorate or staff (J2). Raw data or pre-exploited information was collected, exploited, sanitized and disseminated as intelligence through formal channels. The intelligence was then released on a "need to know" basis to a defined set of "end users." In the past these end users were intelligence staffs for national and coalition commands. The operational commander, as well as other non-military end users sere secondary. As gate keepers, the intelligence staffs distributed "current" intelligence based upon commander objectives and security classification. By the time this "current" intelligence was made available to the operational community; it could be several days old. Today's battlespace operates in near real time (NRT). As such it cannot be fully supported by this traditional intelligence. What is needed is intelligence that is accurate, actionable and available to commanders both planning and executing their tasks.

Within the JFC/CJTF, a class of NRT capable intelligence gathering and dissemination systems already exits. These systems, collectively known as Intelligence Surveillance and Reconnaissance (ISR), provide key capabilities for intelligence collection, exploitation and dissemination.

In order to employ forces efficiently the commander should engage in predictive battlespace awareness (PBA) prior to assigning forces to missions within the area or operations (AO). PBA is defined as the state of awareness achieved and maintained by the commander providing the ability to correctly anticipate future conditions, focus ISR assets, shape the battlespace, and drive an adversary to a course of action (COA) that supports the commander's campaign objectives [Piccerillo et al, 2003]. PBA consists of both the commander's objectives and intent supporting the process of intelligence preparation of the battlefield (IPB). By employing PBA the JFC/CJTF provide the objectives that guide ISR systems within the AO.

2.0 THE ISR SYSTEM

ISR is one of aerospace power's oldest mission areas, dating back to the use of balloons to observe the adversary during the French Revolution. One of the first missions of the airplane was observation. Today, like in the past, we observe and analyze the meaning and impact of a wide variety of events and convey useful, timely intelligence on our adversaries' capabilities and intentions to our commanders [AFDD 2.5.2, 1999].

The fundamental responsibility of ISR is to provide intelligence information to decision makers at all levels of command to give them the fullest possible understanding of the adversary [AFDD 2.5.2, 1999].

By providing commanders and staffs with NRT and archived data and information on the battlefield, the operational commander can plan operations more efficiently and react to adversary actions with appropriate forces in time to blunt operations against own troops.

2.1 ISR Support to Military Operations Other Than War

ISR support to MOOTW requires multi-disciplined, all-source, "fused" intelligence. Manned and unmanned aerial intelligence sensors, to include space-based, can provide valuable information where other intelligence infrastructure is not in place. Remote sensing systems can provide information on terrain, weather and other environmental factors essential to MOOTW. Data from space systems can be used to update antiquated maps and provide up-todate locations of facilities and obstacles. Sensors on space and aerial platforms can also monitor terrestrial force movement and assist in treaty verification [JP 3-07, 1995]. This is especially important in areas where communications and power infrastructure has been destroyed by natural disasters or insurgent and/or criminal activity.

Specific essential elements of information which drive collection management process in MOOTW may differ in focus from those targeted in war. In war, intelligence collection includes an entire range of factors with a major emphasis on the enemy's military capability. Intelligence collection in MOOTW, however, might require a focus on the understanding the political, cultural, and economic factors that affect the situation [JP 3-07, 1995]. This does not mean however, that intelligence products will be substantially different. The exploitation of electro optical/infrared (EO/IR), ground moving target indicator (GMTI) and electronic intelligence/electronic support measures (ELINT/ESM) will largely be the same for MOOTW and conventional/special operations. The primary difference will be in the tasking agency and the end users. For civilian operations, these may be non-governmental organizations (NGO) such as the Red Cross/Red Crescent or civilian governmental agencies such as the US State Department. These organizations and agencies may be seen as surrogate commanders; providing objectives and tasking for military ISR assets. In fact, if done correctly and efficiently, military ISR systems participating in MOOTW operations should notice little if any change to their collection requirements.

2.2 ISR System Classes

ISR systems can be organized into "classes" based upon their products; that is, the data and information they provide. These products include GMTI data, EO/IR and SAR imagery as well as ELINT/ESM information just to name just a few. When tasking a system to fulfill a collection requirement, the commander's intelligence staff must take into account the class or type of ISR system to be utilized. For example, a GMTI system may not be well placed to provide details on the current disposition of an airfield. Similarly, an ELINT system is not the best option for the detection and reporting of vehicle movement within an AO [Mahaffey, 2003].

Within these classes, ISR systems provide varied levels of capability. For example, a deployed commander may have access to imagery from EO systems present on a medium altitude long endurance (MALE) Uninhabited Aerial Vehicles (UAVs) such as the RQ-1 Predator and on hand-launched low altitude short endurance (LASE) UAVs such as Desert Hawk. Both systems provide imagery, but are employed differently. In this case the Predator may support the commander's intelligence staff with imagery of pre-planned and time sensitive targets over a corps wide AO. The Desert Hawk on the other hand, may be employed by the operations directorate strictly in defense of a point target such as an airfield or mobile headquarters. The imagery provided by both systems however, may support a number of other commanders. When this imagery is made available to the network, multiple intelligence and operations staffs as well as other agencies and commands interested in the AO may benefit supporting a wide variety of missions and operations.

Figure 1 depicts a theater-wide set of ISR systems and capabilities. Note that within this notional theatre ISR systems are located on the ground, on the sea, in the air and in space. Further, these systems include the full range of capabilities from highly complex aerospace systems to Special Forces on the ground behind enemy lines. The network these systems connect to must be flexible enough to accept the ISR data and information feeds required by the supported commander, secure enough to protect sources and systems and reliable enough to operate in any condition, world-wide.

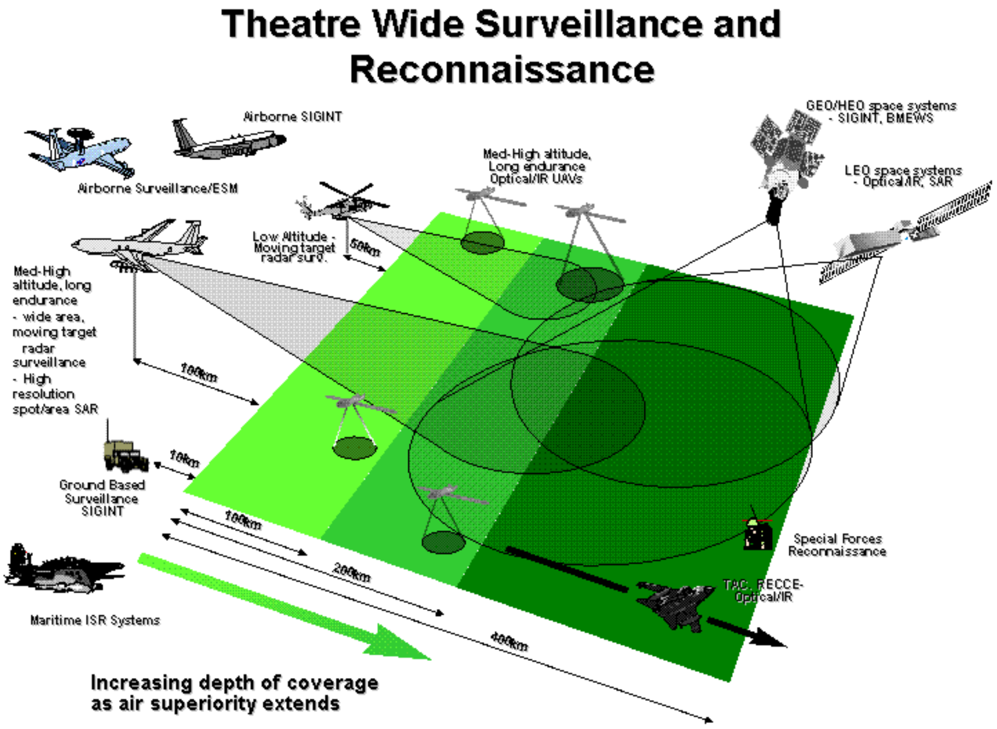
Theatre Wide Surveillance and Reconnaissance
Airborne SIGINT
Airborne Surveillance/ESM
Med-High altitude, Long endurance Optical/IR UAVs
GEO/HEO space systems - SIGINT, BMEWS
LEO space systems - Optical/IR, SAR
Low Altitude - Moving target radar surv.
50km
Med-High altitude, long endurance - wide area, moving target radar surveillance - High resolution spot/area SAR
100km
10km
Ground Based Surveillance SIGINT
100km
200km
400km
Special Forces Reconnaissance
TAC. RECCE- Optical/IR
Maritime ISR Systems
Increasing depth of coverage as air superiority extends

Figure 1: Theatre Wide ISR Systems.

The increase of ISR systems at the operational and tactical level provides not only significant additional capability, but increased complexity as well. Further complicating the employment of ISR systems is the development of these systems in the coalition environment. Heretofore, few nations could provide these assets. These systems were provided to a coalition with very limited access to actual data and imagery. Generally the data and imagery was collected, analyzed, sanitized and disseminated by the owning nation with little appreciation of coalition exploitation needs.

Finally, these systems may provide NRT data and information via system specific data links, common data links (link 16) or by voice. In some cases, these systems may only be capable of providing their data and information post-mission through the formal intelligence phase I and II analysis and exploitation process. Furthermore, their data, because of the sensitivity of their systems, is controlled by both national and coalition agencies and commands. This will further increase the amount of time required to disseminate their data and information.

2.3 The ISR System Revolution

Employment of an ISR system is both complex and expensive. ISR mission requirements are both system specific and vary greatly by type and class. These systems may require specialized capabilities to receive, exploit and disseminate their data. Since the end of the cold war and the advent of coalition operations under United Nations (UN) and NATO flags, there has been a steady change in the accessibility and employment of national ISR systems. These changes have been both operational and technical.

Operationally, few nations can “go it alone” for the myriad of military operations involving large force objectives (i.e. Operation Iraqi Freedom), international peace enforcement (i.e. Operations in the Former Yugoslavia) and natural disaster relief (i.e. South Asian Tsunami Relief), that are becoming the norm as opposed to the exception. Further, ISR systems are now being employed in roles previously unplanned for. An IR system may provide cueing and identification of enemy armor on the move into a combat zone or the location of survivors trapped by an avalanche in the mountains. Essentially, the data and information is the same, the employment is different.

Technically, changes to the employment of ISR data and information can best be described as dizzying. The development of high speed information technology (IT) coupled with increasingly capable communications networks have provided the basis for an ISR system that is characterized by higher speed collection, analysis, exploitation and dissemination of both NRT and archived data and information. These networks cross doctrinal and national lines rendering the old model of ISR as a J2 only asset, archaic and flawed. Additionally, networks previously employed for non-intelligence functions are being employed to provide access to ISR data and information, either directly or as a surrogate system. These include but are not limited to data links (Link 16) as well as network and web enabled data bases and exploitation tools.

As a result, a multitude of commanders and agencies now have access to NRT and archived ISR data and information for both the planning and execution of their operations. Essentially, more and better ISR systems are available; the goal of persistent surveillance within an AO is no longer a concept, it is a reality. For example, in some operations, specific geographical and electronic areas of the AO may be under surveillance 24 hours a day, seven days a week.

On the surface this would appear to be a positive development with no “down side”. In a perfect world, this of course would be true. Unfortunately, the addition of capabilities, commands and other end users has revealed a whole new group of challenges for the ISR system and the commands that operate and employ them in a coalition environment.

2.4 The Coalition ISR Problem

The Coalition ISR problem is multifaceted. First, coalition ISR systems must respond to the requirements of the supported commander. In a coalition this may include more than one commander across more than one component. In these cases the importance of clear objectives by the JFC/CJTF cannot be overstated. Without these objectives, coalition ISR systems will become over-tasked with competing requirements from commanders within and outside of their network.

Second, the data and information produced by the coalition ISR system must be accurate, timely and actionable. The requirement for accurate and timely ISR data and information is a given, but actionable may mean something entirely different. Actionable ISR data and information refers to the applicability of that data and information for employment by the supported commander. Essentially, the data and information must provide support to the commander’s operations or it is simply superfluous and a waste of time and resources. This requires significant and clear input from the supported commander in the form of effective and realistic collection requirements designed to support the commander’s objectives.

Third, as previously reported, ISR data and information is generally protected by the owning nation. There are several reasons for this but most come down to a national desire to protect expensive and complex ISR system capabilities from disclosure to adversarial forces. Disclosure of these capabilities could result in an adversary’s development of counter capabilities thus rendering the system incapable of providing the service it was procured for. As a result, nations are reluctant to disseminate raw or pre-exploited data and information gathered by their ISR systems.

Fourth, a truly joint ISR system will provide capabilities at all levels of command, strategic, operational and tactical. This describes a distributed ISR capability or network. The distributed ISR capability, conducted from multiple independent nodes within an intelligence network, facilitates and enhances accomplishment of JFC/CJTF objectives [JP 2-01, 2004]. Within these levels of command, components also maintain capabilities to support specific operational and/or tactical commanders. For example, the RQ-4 Global Hawk provides data and information to a wide ranging group of supported commanders, but the system normally takes its tasking from the J2 through the Joint Forces Air Component Commander (JFACC). The French Army Hélicoptère d'Observation Radar et d'Investigation sur Zone (HORIZON) system provides support to a Brigade or Division G2 through the Land Component Commander (LCC). Both systems provide Ground Moving Target Indicator (GMTI) and both systems respond to a collection plan. The difference is primarily with their supported commander. Without a joint network of interoperable systems, these ISR systems would continue to support a narrow group of commanders. By employing data links and network enabled databases, these systems can provide these resources to a much larger array of commanders and agencies. In order to ensure efficient employment of these systems, the development of both operational and technical capabilities for the tasking, allocation and dissemination of ISR data and information across components and command levels is required.

Finally, all of these systems produce data and information for dissemination across communications networks to their supported commanders. This can bring up the problem of too much data, not enough information. The availability of the large volumes of data and information may drive requirements that are both un-necessary and un-realistic given network limitations such as bandwidth and security.

Not every commander and agency on the network requires every piece of ISR data and information. Access control of the information may provide some degree of relief for this problem but could in turn reduce the availability of the information during time sensitive operations such as Theatre Missile Defense (TMD) and Suppression of Enemy Air Defenses (SEAD). Operational solutions through the implementation of procedures will also help but require the ability to provide communications between the system's commanders and other end users.

Dissemination of ISR data and information in a coalition environment is a complicated and multifaceted problem. In order to address this problem effectively a systemic approach to ISR data and information dissemination is required. This systemic approach must regard the ISR system as a whole, a system of systems, serving multiple commanders and agencies.

3.0 A GLOBAL APPROACH TO ISR DATA AND INFORMATION DISSEMINATION

How do ISR systems supporting a JFC/CJTF operation provide their data and information through common modes of communication and within the bounds of national and coalition system security to the maximum number of supported and supporting commanders rapidly and efficiently? The answer lies within the creation of net-centric and net-enabled capabilities supporting multi-level data dissemination across operational command architectures. There are a number of potential solutions. All involve a network of some type. The following paragraphs provide a discussion of these options. Note that this list is not exclusive and that some capabilities will be added as they become technically and operationally available.

3.1 Network Centric ISR Systems

What exactly is a network enabled system? Like all buzz words, the term net enabled or web enabled mean different things to different users. Network-centric capabilities allow the force to attain an improved information position that can partially "lift the fog of war" and enable commanders to improve their decision making and fight in ways that were not previously possible [NCW, 2001]. All network-centric concepts share the same simple idea that information sharing is a source of potential value. Network centric concepts enabled by the networking of various elements of the force; the network alone is not sufficient to generate increased combat power, but it is the primary medium for enabling NCW concepts [NCW, 2001]. The systems operating within these networks must share common values such as data format and transmission medium. A system joining the network without adherence to established common values will not be fully interoperable and may impede the network as its data and information is disseminated to and ultimately discarded by members of the network. The utility of these ISR systems can be maximized by integrating them into a network enabled capability ISR system to meet the commander's collection and targeting requirements [CAESAR TTP 5.3, 2003].

As ISR systems are designed, there should be emphasis on as many collectors as possible to capable of transmitting what they sense through a network centric architecture. This network centric architecture links sensors, decision-makers, and shooters to obtain information superiority in which translates to generation of combat power [Bush, 2001].

Experimentation by the Coalition Aerial Surveillance and Reconnaissance (CAESAR) program is providing network-centric solutions based upon an integrated system of nationally owned ISR systems providing GMTI data, SAR imagery and products derived from the exploitation of their primary products. While these solutions are based in GMTI, SAR and Link 16, they provide broad application for a variety of ISR capabilities, particularly in among the class of ISR systems that comprise Aerospace Ground Surveillance and Reconnaissance (AGS&R).

The flowing paragraphs will focus on the advances made in the dissemination of net-centric ISR data and information using results of Joint War-Fighter Interoperability Demonstration (JWID) 2004 as well as the CAESAR Simulation Exercise (SIMEX) 2003, and the JTIDS Operators Tactics Meet (JOTM) 2004. Included in the discussion are current and future initiatives for the implementation of ISR data and information across a broad spectrum of commanders. Note that information gained the during this experimentation is fully applicable to operational and future NATO programs C2 and ISR programs such as the NATO Air Command and Control System (ACCS) and the Alliance Ground Surveillance (AGS) capability and in the development of the NATO Network Enabled Capability (NNEC) as well as the NATO Joint ISR (JISR) initiative.

The CAESAR project has developed both operational and technical capabilities to disseminate and exploit AGS&R data and information between national and coalition C2 and ISR systems on dedicated local/wide area networks (LAN/WAN), data link (Link 16) and via the world wide web. These capabilities are serving as the basis for the development of NATO and national procedures and systems for C2ISR operations in the coalition environment.

3.2 Network Enabled System Requirements

The joint intelligence communications sub-architecture encompasses collection, processing, exploitation, analysis, and dissemination nodes. These nodes are supported by a robust communications infrastructure and automated systems equipped with tailored applications to meet the broad array of intelligence activities [JP 2-01, 2004]. These nodes in turn comprise the network on which ISR systems must collect and disseminate data and information. Typically, ISR data can be transmitted in NRT to suitably equipped and network enabled ground stations for processing and exploitation. Some systems broadcast this data to a large number of receivers, while others use point-to-point links to send the data to only one ground station. When correctly connected to a wide area network (WAN), ISR systems, both airborne and ground based may provide raw or pre-exploited and exploited ISR data and information to air and ground based C2 systems via numerous network enabled data bases [CAESAR TTP 5.3, 2003].

However, the network is not enough; in order to join the network, a system must meet a set of minimum standards. For the CAESAR project, these standards were both operational and technical. Operationally, CAESAR systems were required to adopt formats and procedures as directed by NATO directives and regulations. This provided the framework for the further development an interoperable capability. Since ISR systems primarily serve the intelligence staff, the primary directives employed were BiSC 65-5 (Collection Management) and BiSC 80-70 (Synchronization [Targeting]). Where NATO directives and regulations were not available national directives and regulations were employed. Because the CAESAR project provided new concept of interoperable ISR systems, some capabilities were realized that were not covered by NATO or national directives and regulations. In these cases, local procedures were developed and subsequently passed to NATO commands and agencies for inclusion in future directives and regulations.

In order to ensure technical interoperability, CAESAR participants were required ensure their systems were compliant with NATO Standard Agreements (STANAGs) on data format and dissemination. This provided a basis for the development and implementation of an integrated common ground picture made up of GMTI and Link 16 data, SAR imagery and ISR management tools.

Of note, there is a danger in the unfettered race towards the development of networks. When the network becomes the objective, the emphasis may evolve to getting networks in place so as opposed to getting the right data to the right commander. While even the best intelligence is only useful if it is communicated, poor data on the network can also have devastating consequences. One potential danger is that the flow of information, regardless of the quality of that information, may become a measure of success. Particularly if the number of contributors to the intelligence networks grows, possibly exponentially, the data must still be analyzed and validated [Chizek, 2003]. For this reason the emphasis must remain on the collection, exploitation and dissemination of accurate and actionable ISR data and information as opposed to the network.

3.3 Multilayered ISR Networks

The 21st century war-fighter has access to multiple networks. These networks include the traditional WAN/LAN that exists at most commands. Within NATO this could be desribed as the CRONOS system, in the US; this could be described as SIPRNET. If dedicated secure networks are not already in place, they can be created through the use of telecommunications internal to the command. This can be done by building and/or contracting dedicated communications architecture and providing secure crypto capabilities at the transmitting and receiving nodes. Given enough bandwidth and security, the coalition LAN/WAN may provide access to the dissemination of ISR data and information through standard ISR workstations. In this case, raw or pre-exploited data and information may be made available from the ISR system to a larger group of commanders for analysis and exploitation.

When limited bandwidths reduce the ISR system's ability to transfer large files such as imagery and streaming video between ISR nodes, technical and operational prioritization procedures for applications and data provide potential solutions for the optimal usage of limited network bandwidths. The applications or data types may have various levels of priority for data delivery. These applications should consider both technical and operational aspects of the ISR mission. For example, GMTI and ESM data are generally available in NRT and are perishable as intelligence products. These products are often used by operators and analysts to determine NRT operations such as the viability of lines of communication as well as the location and movement of adversary forces. This data can be used for phase I and II intelligence processing such as battle damage assessment and pre-planned targeting. However, its greatest value has traditionally been in NRT support of the operational commander. Imagery on the other hand, is often used in phase I and II analysis of intelligence data and information collected in NRT and archived over a period of time. Imagery may be employed in NRT combat operations but has historically been less critical to NRT operations than GMTI, ESM and aerospace surveillance. In general, if a limited bandwidth network supports message prioritization, low bandwidth data such as GMTI should be given the highest priority because it is used extensively by NRT users and it occupies less space than imagery. Imagery tends to be used more by intelligence analysts and is may not be as time-sensitive [SADP 4.0, 2004]. In this case, operational procedures governing the dissemination of certain files are critical to the efficient operation of the "global" ISR system on the WAN/LAN.

Other networks include data link and text transfer via voice and telecommunications. Data link may act as a surrogate for ISR data by providing a location, time and amplifying information about targets of interest in the AO. Data link information may act as a trigger for ISR systems to cue their systems to in search of identification for adversary forces or may provide identification of targets of interest being tracked in the AO. For example, the E-8C Joint STARS may detect and track stationary GMTI. Stationary GMTI is radar data indicating movement that is static within the AO. Stationary MTI may include among other things, a rotating radar antenna. This track may then be employed by the Nimrod R1 as a reference point for the detection and triangulation of radar signals within the AO. In this case, the Nimrod R1 may provide identification of the track remotely.

While the data link can provide ISR data and information to a wider array of commanders and agencies, there are several problems to be considered. First, data link data is generally not accurate enough for targeting. It can however, provide cueing as well as battelspace awareness for the employment of further ISR resources against track. Second, not every participant within the data link network has the same implementation of the data link message group. For example, the Link 16 J 3.5 ground track may be displayed differently by JSTARS, the E-3 and combat weapons systems such as the F-16. Each system may or may not display a track number, the identification of the track in once system may be different in another and the amount and type of amplifying information (i.e. track quality) may be displayed differently or not at all between systems.

Text or voice networks provide the ability to work around integration and interoperability issues caused by network and/or system interoperability and integration non-compliance. These options include free text messaging via CHAT functions, e-mail and telecommunications including radio, telephone and facsimile. Text messaging may take the place of automated network centric ISR capabilities or may supplement these capabilities with amplifying data and information. Indeed, a completely integrate common operating picture may have elements of all network centric, data link and textual dissemination of data and information running simultaneously providing ISR data and information to a number of supported and supporting commanders. The key is the management of these capabilities to provide the maximum integrated capability with a minimum of conflicts between systems at the technical level and commands at the operational level.

3.4 Variable Interoperability – Exploiting the Lowest Common Denominator

Interoperability is a key component in the employment of network centric ISR systems. As previously noted, these capabilities may run the gamut, from fully interoperable systems on a WAN/LAN to transfer of data and information via textual formats over a radio frequency.

In coalition operations, variable levels of technical and operational interoperability results in the need for a sliding scale of interoperability that capitalizes on the most interoperable systems while allowing for the integration of the least interoperable systems. While this task is difficult, it is not impossible. By finding the lowest common denominator among the coalition partners, the commander can set a baseline of interoperability that includes all systems. For example, some ELINT systems are only capable of voice relay while on-station. Integration of these valuable assets requires a radio frequency to receive data and information. Ideally the information collected on this frequency will be placed into an integrated network by a partner ISR system as a data link track or a text report. This information may then be forwarded to network enabled databases for further exploitation as required.

Small UAVs below brigade level are another source of this information. These systems provide EO/IR capabilities for their workstation operators at their individual headquarters. Unfortunately, many of these workstations are either not network enabled or cannot connect to a secure network with enough bandwidth to disseminate their data and information. As with the ELINT system above, these systems may only be able to provide textual reporting in NRT and data and information post mission through download to media such as CD or DVD. This media can then be placed on a secure database when capabilities exist.

4.0 CONCEPT DEVELOPMENT IN THE OPERATIONAL ENVIRONMENT

Before a concept can become an operational solution it must first be validated in an operational environment. For coalition ISR systems this is a complicated task. Some ISR systems such as the RC-135 Rivet Joint, the E-8C Joint STARS and the RQ-1 Predator are already operational. Their capabilities and limitations are well documented through operational lessons learned and current tactics, techniques and procedures (TTPs). Some ISR systems can be classified as "near term operational." These systems are expected to be operational within the next one to five years; an example of a near term operational system is the UK Airborne Standoff Radar (ASTOR) ground surveillance system. Because ASTOR is nearly operational, planning for operational and technical interoperability may commence in an effort to ensure a smooth transition from developmental to operational status. Some ISR systems may be characterized as "long term operational." These systems are currently under development and are expected to become operational in more than five years. An example of this system is the NATO Alliance Ground Surveillance (AGS) system. AGS is due to meet initial operational capability (IOC) in 2010. As a result, the benefits of integrating the system into an operational network are negligible for near term operations but is essential to the maturity and integration of the system prior to IOC. Finally, there are some systems that will not become operational as stand-alone capabilities but will be integrated into operational systems, both near and long term. An example of this system is the Motion Analysis, Tracing and Exploitation (MATrEx) auto-tracking system. MATrEx, while not designed as a stand alone capability, is intended to be integrated into other operational systems providing an automated ground tracking capability.

Because, integration of these systems into a C2ISR architecture requires validation in an operational environment, experimentation during live and simulated events with operational commanders and units is essential. Since 2001, the CAESAR project has participated in a number of live and simulated exercises. Note that these exercises were not specifically designed to provide validation of developmental ISR capabilities. However, the addition of robust C2 elements and processes as well as other non-ISR systems provided both operational validation of ISR concepts and education of supported commanders regarding current and near term ISR system capabilities. The results of these experiments were then integrated into NATO directives, regulations and STANAGs for future employment.

4.1 Experimentation in the Operational Environment

The following paragraphs detail a number of exercises and experiments in which CAESAR ISR concepts and capabilities were employed. These were accomplished under the auspices of the NATO Consultation, Command and Control Agency (NC3A) and other national participants. These results are representative of ISR capabilities provided by AGS&R systems operating within a multilayered architecture networks.

4.2.1 Coalition Experimentation

The focus of CAESAR experimentation during Joint War-fighter Interoperability Demonstration (JWID) 2004 was directed at capabilities developed and implemented by the CAESAR project. Specifically, JWID 2004 involved the operational evaluation and validation of net-centric methods of AGS&R ISR data and information dissemination. Experimentation for net-centric AGS&R ISR data dissemination JWID 2004 was subdivided into three primary areas. These included and integrated C2ISR system employing Link 16 as the primary vehicle of transfer, the development of network and web enabled databases for ISR products employing the coalition shared database (CSD), and the implementation of network centric capabilities enabling cross domain information transfer employing two secure networks in the coalition environment. The findings of these experiments have proven the ability to provide both ISR data and information to a wider array of end-users not traditionally associated with an established intelligence network.

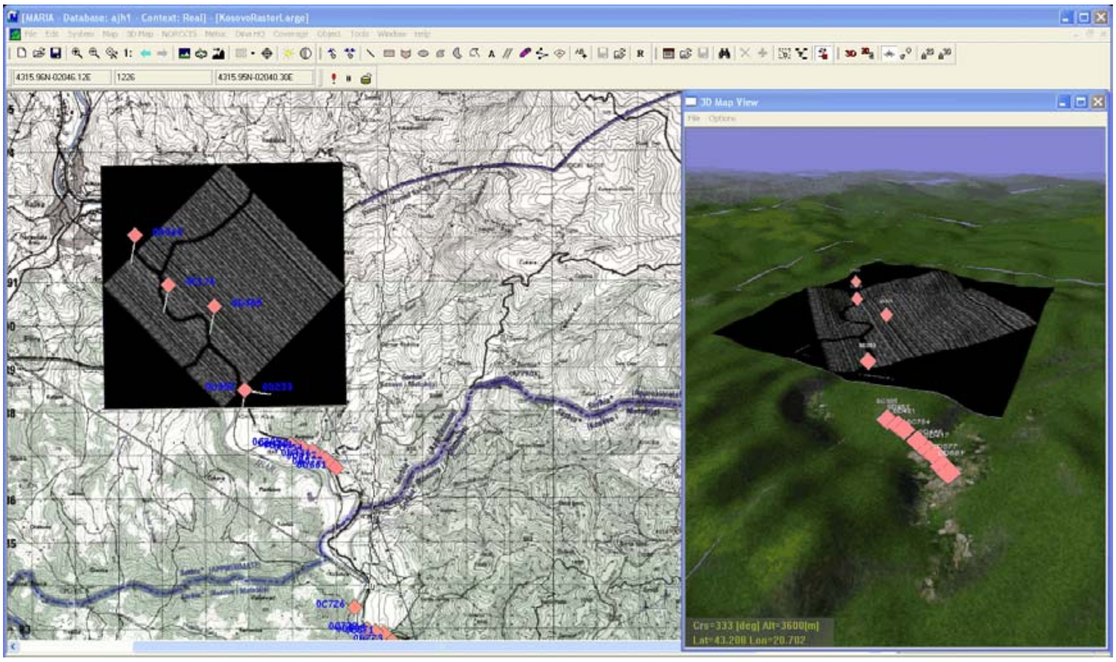
[MARIA - Database: ajh1 - Context: Real] - [KosovoRasterLarge]
File Edit System Map 3D Map NORCCIS Metoc Data HQ Coverage Object Tools Window Help
4315.96N-02046.12E
1226
4315.95N-02040.30E
3D Map View
File Options
Crs=333 [deg] Alt=3600[m]
Lat=43.208 Lon=20.702

Figure 2: ISR Data and Integration – NORCCIS.

Employment of Link 16 for ISR data and information provides a common conduit for the dissemination of ISR data and information to commanders and systems with limited access to a dedicated LAN/WAN. This is especially true for C2 Systems such as the Norwgian Command and Control Information System (NORCCIS) and the Integrated Command and Control System for Air Operations (ICC) for NATO. These systems may not display ISR data in its raw or pre-exploited form. In these cases, Link 16 tracking can provide cueing and situation awareness to the commander and staff through the visual display. Figure 2 depicts the NORCCIS system displaying an integrated picture of Link 16 tracks and SAR imagery. Of note, this capability, validated in JWID 2004 is currently operational with Norwegian Defence Forces.

During JWID 2004, the Link 16 picture provided only part of the commander's COP. In order to fully exploit the CAESAR capability, an integrated C2ISR COP needed to be implemented. This capability provided a both a visual reference of data and information for the commander as well as capabilities designed to manage the employment ISR systems within the AO. These collection management tools allowed the commander and staff to modify current ISR collection requirements as well as plan for dynamic tasking of ISR assets both prior to and during the mission. Figure 3 provides a visual representation of these tools. Note that the collection plans and system orbits are prominently displayed for the use of the system operator.

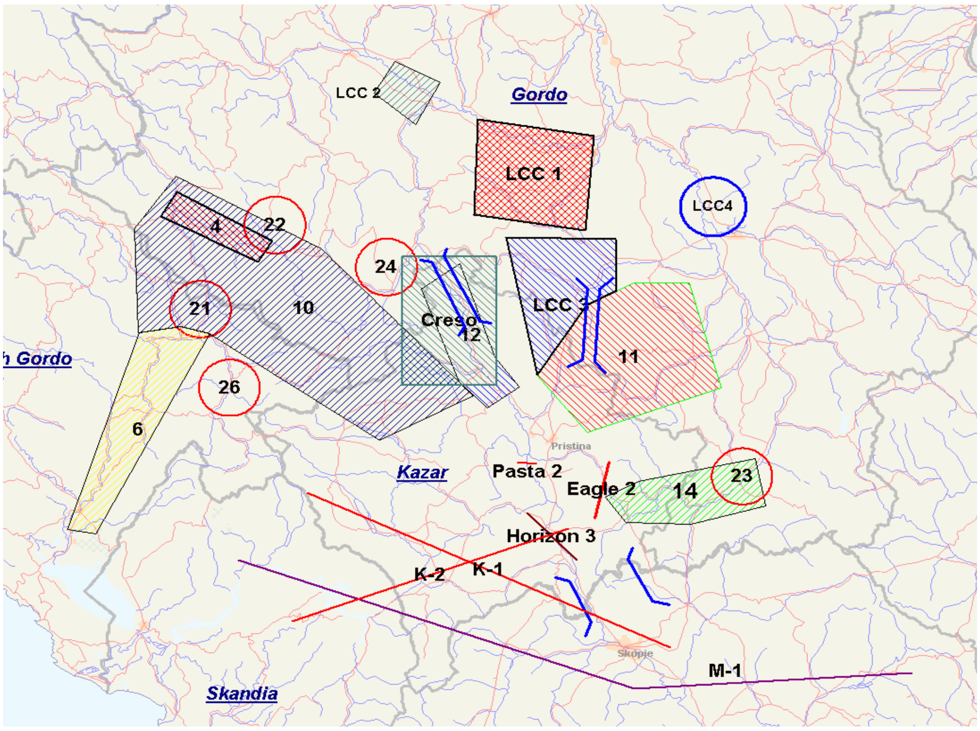

Figure 3: ISR System Collection Requirements.

Cross domain C2ISR dissemination has long been a critical requirement for coalition operations. Because these national ISR systems provide highly classified information the networks they reside on are secure. Because these networks are protected, nations, even those within a coalition are often hesitant to allow coalition systems access to their secure networks. Unfortunately low number of ISR systems coupled with the high demand of commanders and agencies for ISR data and information require a rapid, accurate method of dissemination. For some missions such as Time Sensitive Targeting (TST), the ability to search and retrieve data cross domain would be critical to mission success. During JWID 2004, ISR data was successfully disseminated between secure domains through the use of the Information Exchange Gateway (IEG). The IEG allowed the blue and red coalitions to determine the type of data to be transferred between secure domains. The IEG accomplished this by monitoring the data and information as it moved through a series of ports. In order to be successful, the data and information had to be encapsulated in an XML format. Figure 4 depicts the architecture in which two CSDs, one on the red (NATO) network and one on the blue (Coalition) network were able to share ISR data and information. Further, other end users on the red network were able to query and retrieve data from the blue CSD through the red CSD. This capability provides a potential solution to coalition cross domain data and information dissemination.

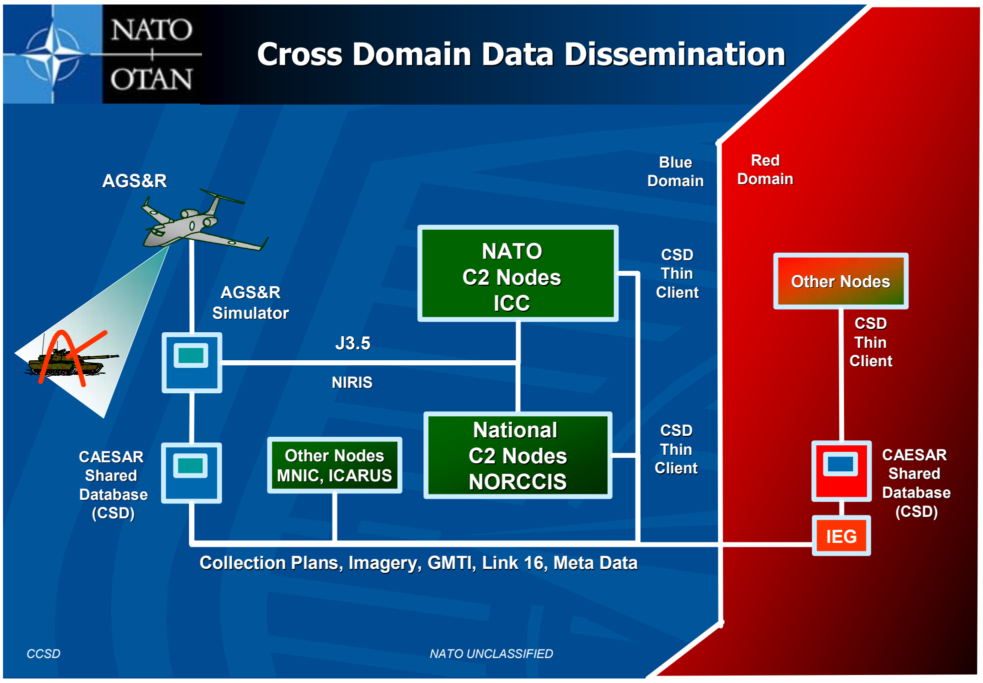

Figure 4: Cross Domain ISR Architecture – JWID 2004.

4.2.2 Operational Validation

JWID 2004 was a coalition based experiment no operational scenario to validate these capabilities against. Since the focus of the experiments was the validation of alternate means of data dissemination, primarily through Link 16 and web enabled CSD, an operational exercise dedicated to these capabilities was required. The JTIDS Operators Tactics Meet (JOTM) 2004 provided this opportunity. For JOTM 2004, NC3A would provide live ground tracks for transmit to an operational network. These tracks would be received and exploited by C2ISR systems including E-3 Sentry Airborne Early Warning and Control (AEW&C) aircraft from NATO, France and the UK, as well as Link 16 equipped F-16 fighter aircraft from Belgian and Danish Air Forces. These systems were to receive, exploit and engage these tracks in accordance with their rules of engagement. In order to guarantee a realistic operational picture, NC3A planned to instrument target vehicles on the range, reporting their position to a simulator at NC3A, then transmitting the ground tracks via an operational Link 16 node and via WAN to NAEW E-3 component at Geilenkirchen AB GE. Figure 5 depicts the NC3A JOTM 2004 network. During live operations, both AEW&C and F-16s received and engaged the targets. JOTM 2004 was successful in validating the AGS&R system's ability to receive, exploit and disseminate ISR data and information using the Link 16 network.

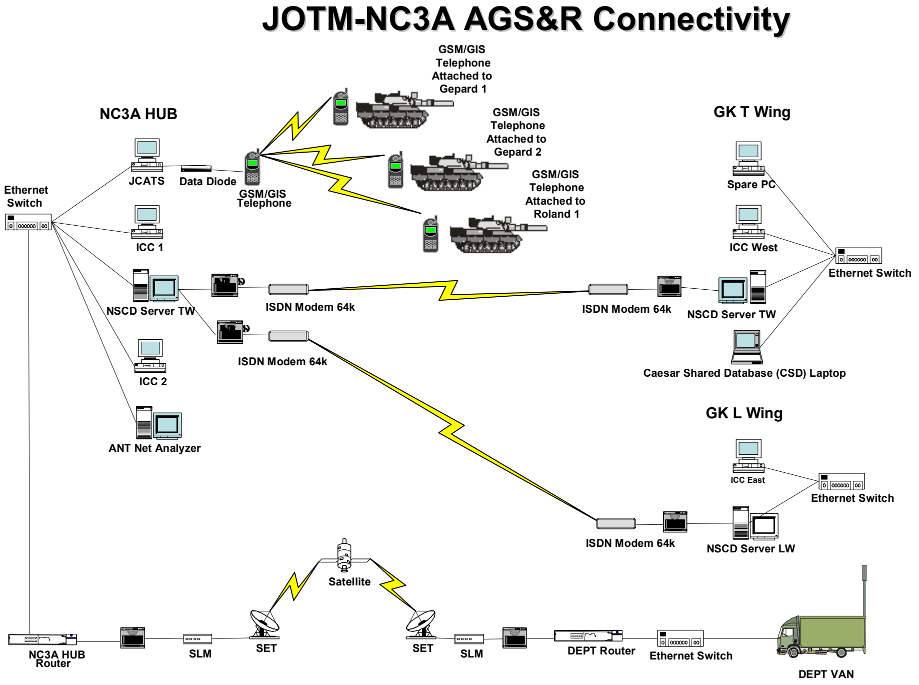

Figure 5: JOTM 2004 – NC3A AGS&R Connectivity.

Validation of the CSD is somewhat more problematic. Essentially, as a developmental capability it still requires extensive technical experimentation and integration. As an operational capability however, it requires a scenario driven exercise with a defined set of operational objectives. For this reason, a small scenario was created during the CAESAR Technical Interoperability Experiment (TIE) 2004. During TIE 2004 operators from the various nations and workstation experimented with the CSD using a portion of the CAESAR SIMEX 2003 scenario. The plan was to review operator procedures for employment of the CSD as a network enabled ISR data base as well as a theatre collection management tool for assigned ISR assets. The results of TIE 2004 detailed potential areas of improvement in the development and implementation of operator procedures as well as discovery of new methods for the dissemination of ISR information through alternate means.

TIE 2004 provided the first opportunity to implement and use a CHAT capability between individual systems across a network. During the TIE, ISR workstation operators were extremely enthusiastic about using instant messaging as a means of communication with other workstations and CAESAR participants. They would like to see this technology further implemented in future exercises/experiment [TIE, 2004].

Disciplined employment of CHAT reduced the bandwidth requirements by pointing operators to the CSD for new data and information. This allowed the system to adopt a “pull” versus “push” concept for large imagery files such as SAR. Previously large images being “pushed” though the network exceeded the available bandwidth. By using CHAT to alert system operators that new imagery was available on the CSD, the operators could go to the CSD, view thumbnails of the imagery and decide what if any of the imagery was needed. Other CHAT based ISR management functions included the ability to send a sensor service request (SSR) and system reports such as joining reports, mission reports and the Size Activity, Location and Time (SALT) report. By employing CHAT for these functions, bandwidth requirements were reduced while opportunities for receipt and acknowledgment of system requests and direction provided increased efficiency in the overall management of the ISR system.

5.0 TRANSITION TO THE WAR-FIGHTER

The development of integrated and interoperable ISR systems is incomplete without a plan to transition the capabilities into the active force. The CAESAR nations are responsible for transition of the capability at the national level. As a result, the implementation of the capability has been uneven at best. Currently, only Norway has fully transitioned the CAESAR capability through the implementation of a CSD for NORCCIS. Other nations are transitioning thee capabilities as their developmental ISR systems become operational. More importantly, the technical and operational procedures and capabilities derived from the CAESAR Project are being implemented in a follow-on ISR interoperability project. This project, known as the Multi-sensor Aerospace/Ground Joint Interoperable ISR Coalition (MAJIIC) will build upon CAESAR successes adding EO/IR, streaming video and ELINT to the list of ISR data and information classes available as a network enabled system of systems. Furthermore, CAESAR and MAJIIC capabilities and processes are being integrated into the design and development phase of the NATO AGS program as well as forming the basis for the ACE 80-6 Tactical Employment chapter on NATO ISR operations.

6.0 CONCLUSION

The 21st century battlefield presents increasingly difficult intelligence challenges.

Threats now span a widening range of activities: from terrorist use of weapons of mass destruction (WMD) to regional military or social crises that threaten the territorial integrity coalition forces [JP 2-01, 2004]. New and elusive enemies, natural disasters and coalition based operations will be the norm, not the exception for the foreseeable future. Reductions in raw numbers of forces including mission critical ISR assets will require those remaining assets to be deployed more often. Increased capabilities in ISR systems, including network enabled exploitation and dissemination will provide opportunities to increase the efficient employment of reduced ISR assets for a wider array of commanders. Finally, increased capabilities for dissemination of data and information will provide a marked increase in the quality, quality and accuracy of ISR data to commands and staffs not previously able to receive and exploit this information. Without proper capabilities for exploitation and dissemination, this critical information will at best be lost, at worst be subject to misanalyses, potentially leading to engagements of friendly and/or neutral forces and personnel on the battlefield.

In order to better employ these limited assets and their vast quantities of data and information, commands, both national and coalition, must prepare by implementing automated applications for the proper collection, exploitation and dissemination of ISR data and information while developing operational procedures that take advantage of network enabled capabilities while allowing for the full range of capabilities available to the commander. Otherwise, the net centric dissemination of ISR data and information to coalition participants will be effected only through the employment of manual and textual means. In other words, the ISR system of systems will be reduced to a series of telecommunications and textual formats, thereby rendering the technology largely moot for the coalition.

7.0 REFERENCES

[AFDD 2-5.2, 1999]
Air Force Doctrine Directive 2-5.2, Intelligence Surveillance and Reconnaissance Operations, 21 April 1999

[Bush, 2001]
Bush, Bichson Intelligence Surveillance and Reconnaissance (ISR) Support to Urban Operations, A Monograph, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, First Term AY 00-01

[CAESAR TTP 5.3, 2004]
GMTI/SAR Capable ISTAR Tactics Techniques and Procedures, Operations Working Group, Version 5.3, July 23, 2004

[Chizek, 2003]
Chizek, Judy, Report for Congress, Military Transformation: Intelligence Surveillance and Reconnaissance, Updated January 17, 2003

[JP 2-01, 2004]
Joint Publication 2-01, Joint and National Intelligence Support to
Military Operations, 7 October 2004

[JP 3-07, 1995]
Joint Pub 3-07, Joint Doctrine for
Military Operations Other Than War, 16 June 1995

[Lee, 2004]
The Coalition Aerial Surveillance and Reconnaissance (CAESAR) technical integration experiment 2004 (TIE04) lessons learnt report – Operations working group (OWG) perspective 4-15 October 2004

[Mahaffey, 2003]
Mahaffey, John, Observations in allocation and tasking of Joint level Intelligence Surveillance and Reconnaissance (ISR) systems in support of Coalition Operations, June 2003

[NCW, 2001]
Network Centric Warfare, Department of Defense, Report to Congress, 27 July 2001

[Piccerillo, et al, 2003]
Piccerillo, Robert, Brumbaugh, David, Predictive Battlespace Awareness: Linking Intelligence, Surveillance and Reconnaissance Operations to Effects Based Operations, 2003

[SADP, 2005]
GMTI/SAR Capable ISTAR System Architecture Design Principles (SADP), Architecture Development Working Group, Version 4.0 Draft A, February 14, 2005

8.0 BIOGRAPHY

John L Mahaffey is a Senior Scientist with the Command and Control Systems Division, NATO Consultation, Command and Control Agency, The Hague, The Netherlands. He provides operational concept analysis and system architecture development for the integration and interoperability programs for multinational C2 and ISR systems and applications. He has more than 23 years of operational and system development experience in ground-based and airborne C2 and ISR systems. His operational experience includes operations in the Middle East, the Balkans, Central and Northern Europe, South East Asia and the Caribbean. He is a retired USAF Major and Master Air Battle Manager with more than 4000 hours on E-3 AWACS and E-8 JSTARS aircraft serving in various weapons control and mission crew commander positions.